AMENDMENTS TO THE CLAIMS

This listing of the claims replaces all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. [Currently Amended] A method of conveying data traffic through a node of a communications network, the method comprising the steps of:

   a) assigning a parameter respecting the data traffic in an ingress interface;

   b) conveying the data traffic and the respective parameter to selected ones of a plurality of ~~an~~ egress ~~interface~~ interfaces, each egress interface having a respective plurality of logical egress network ports; and

   c) in the egress interface, forwarding the data traffic to one or more of the respective plurality of logical egress network ports based on the parameter.

2. [Original] A method as claimed in claim 1, wherein the parameter comprises any one or more of: information identifying the ingress interface; information identifying a quality of service (QoS) of data traffic received by the ingress port; information identifying a DiffServ codepoint of data traffic received by the ingress port; and information identifying a source address of data traffic received by the ingress port.

3. [Original] A method as claimed in claim 2, wherein the step of assigning a parameter comprises a step of evaluating the data traffic to derive a value of the parameter.

4. [Original] A method as claimed in claim 3, wherein the step of evaluating the data traffic comprises a step of assigning a default value of the parameter.

5. [Original] A method as claimed in claim 4, further comprising the steps of:

   a) evaluating one or more layer-specific headers of the data traffic; and

   b) modifying the default value of the parameter based on the evaluation result.

6. [Original] A method as claimed in claim 5, wherein the parameter is a normalized parameter value obtained by successively evaluating each one of the one or more layer-specific headers in turn, and modifying the parameter value based on each successive evaluation result.

7. [Original] A method as claimed in claim 1, wherein the step of conveying the data traffic and the respective parameter comprises the steps of:

a) inserting the parameter into an intra-switch header; and

b) appending the intra-switch header to the data traffic.

8. [Currently Amended] A method as claimed in claim 7, wherein the step of ~~processing~~ forwarding the data traffic comprises stripping the intra-switch header from the data traffic.

9. [Original] A method as claimed in claim 7, wherein the step of conveying the data traffic and the respective parameter further comprises a step of conveying the data traffic through a multicast-capable switch fabric.

10. [Currently Amended] A method as claimed in claim 9, wherein the data traffic and the respective parameter are replicated by the switch fabric to ~~one or more~~ each selected egress interfaces of the node.

11. [Previously presented] A method as claimed in claim 1, wherein the step of forwarding the data traffic in the egress interface further comprises either one or both of: implementing a traffic policing function; and applying a predetermined policy.

12. [Original] A method as claimed in claim 11, wherein the step of implementing the traffic policing function comprises:

a) detecting congestion of the egress interface; and

b) discarding low-priority traffic such that the congestion is reduced.

13. [Original] A method as claimed in claim 11, wherein the policy is defined in respect of the egress interface.

14. [Original] A method as claimed in claim 11, wherein the policy is defined in respect of an egress network port associated with the egress interface.

15. [Original] A method as claimed in claim 11, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

16. [Original] A method as claimed in claim 15, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

17. [Original] A method as claimed in claim 15, wherein the DROP policy is adapted to prevent transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

18. [Original] A method as claimed in claim 15, wherein the TRANSLATE policy is adapted to modify one or more of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

19. [Original] A method as claimed in claim 18, wherein the step of applying the TRANSLATE policy comprises the steps of:

a) querying a translation table; and

b) inserting the query result into the data traffic.

20. [Original] A method as claimed in claim 19, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

21. [Original] A method as claimed in claim 19, wherein the translation table is specific to the egress interface.

22. [Previously presented] A method as claimed in claim 19, wherein the translation table is specific to a logical egress network port of the egress interface.

23. [Currently Amended] A node of a communications network, comprising:

a) an ingress interface adapted to assign a parameter respecting data traffic received over the network;

b) ~~an~~ a plurality of egress ~~interface~~ interfaces having a respective plurality of logical egress network ports, ~~the~~ each egress interface being adapted to forward the data traffic to one or more of its respective plurality of logical egress network ports using the parameter; and

c) means for conveying the data traffic and the respective parameter across the node between the ingress interface and selected ones of the plurality of egress ~~interface~~interfaces.

24. [Original] A node as claimed in claim 23, wherein the parameter comprises any one or more of: information identifying the ingress interface; information identifying a quality of service (QoS) of data traffic received by the ingress interface; information identifying a DiffServ codepoint (DSCP) of data traffic received by the ingress interface; and information identifying a source address of data traffic received by the ingress interface.

25. [Original] A node as claimed in claim 24, wherein the ingress interface comprises means for evaluating the data traffic to determine a value of the parameter.

26. [Original] A node as claimed in claim 25, wherein the means for evaluating the data traffic is adapted to assign a default value of the parameter.

27. [Original] A node as claimed in claim 26, wherein the means for evaluating the data traffic further comprises:

a) means for evaluating one or more layer-specific headers of the data traffic; and

b) means for modifying the default value of the parameter based on the evaluation result.

28. [Original] A node as claimed in claim 27, wherein the parameter is a normalized parameter value obtained by successively evaluating each one of the one or more layer-specific headers, and modifying the parameter value based on each successive evaluation result.

29. [Original] A node as claimed in claim 23, wherein the means for conveying the data traffic and the respective parameter comprises:

a) means for inserting the parameter into a header; and

b) means for appending the header to the data traffic.

30. [Original] A node as claimed in claim 29, wherein the header is stripped from the data traffic in the egress interface.

31. [Original] A node as claimed in claim 29, wherein the means for conveying the data traffic and the respective parameter further comprises a multicast-capable switch fabric.

32. [Original] A node as claimed in claim 31, wherein the multicast-capable switch network is adapted to replicate the data traffic and the respective parameter to one or more egress interfaces of the node.

33. [Original] A node as claimed in claim 23, wherein the egress interface comprises means for implementing a traffic policing function.

34. [Original] A node as claimed in claim 33, wherein the means for implementing the traffic policing function comprises:

a) means for detecting congestion of the egress interface; and

b) means for discarding low-priority traffic such that the congestion is reduced.

35. [Cancelled]

36. [Original] A node as claimed in claim 23, wherein the egress interface comprises means for applying a predetermined policy respecting the data traffic.

37. [Original] A node as claimed in claim 36, wherein the policy is specific to the egress interface.

38. [Original] A node as claimed in claim 36, wherein the policy is specific to a logical egress port associated with the egress interface.

39. [Original] A node as claimed in claim 36, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

40. [Original] A node as claimed in claim 39, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

41. [Original] A node as claimed in claim 39, wherein the DROP policy is adapted to prevent transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

42. [Original] A node as claimed in claim 39, wherein the TRANSLATE policy is adapted to modify one or more of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

43. [Original] A node as claimed in claim 42, wherein the means for applying the TRANSLATE policy comprises:

a) means for querying a translation table; and

b) means for inserting the query result into the data traffic.

44. [Original] A node as claimed in claim 43, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

45. [Original] A node as claimed in claim 43, wherein the translation table is specific to the egress interface.

46. [Currently Amended] A node as claimed in claim 43, wherein the translation table is specific to a logical egress network port of the egress interface.

47. [Cancelled]

48. [Cancelled]

49. [Cancelled]

50. [Cancelled]

51. [Cancelled]

52. [Cancelled]

53. [Cancelled]

54. [Currently Amended] An egress interface of a network node, the egress interface being adapted to send outbound data traffic over a communications network, and comprising:

a) means for receiving data traffic and a respective parameter from ~~an ingress interface~~ a multi-cast capable switch fabric of the node, the multi-cast capable switch fabric being adapted to replicate the data traffic and its respective parameter to a selected one or more of a plurality of egress interfaces of the network node;

b) a plurality of logical egress network ports coupled to the communications network; and

c) means for forwarding the data traffic to a selected one or more of the plurality of logical egress network ports using the respective parameter.

55. [Previously presented] An egress interface as claimed in claim 54, wherein the means for forwarding the data traffic further comprises either one or both of:

a) means for implementing a traffic policing function; and

b) means for applying a predetermined policy respecting the data traffic.

56. [Original] An egress interface as claimed in claim 55, wherein the means for implementing the traffic policing function comprises:

a) means for detecting congestion of the egress interface; and

b) means for discarding low-priority traffic such that the congestion is reduced.

57. [Original] An egress interface as claimed in claim 55, wherein the policy is specific to the egress interface.

58. [Original] An egress interface as claimed in claim 55, wherein the policy is specific to a logical egress port associated with the egress interface.

59. [Original] An egress interface as claimed in claim 55, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

60. [Original] An egress interface as claimed in claim 59, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

61. [Original] An egress interface as claimed in claim 59, wherein the DROP policy is adapted to prevent transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

62. [Original] An egress interface as claimed in claim 59, wherein the TRANSLATE policy is adapted to modify one or more of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

63. [Original] An egress interface as claimed in claim 62, wherein the means for applying the TRANSLATE policy comprises:

a) means for querying a translation table; and

b) means for inserting the query result into the data traffic.

64. [Original] An egress interface as claimed in claim 63, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

65. [Original] An egress interface as claimed in claim 63, wherein the translation table is specific to the egress interface.

66. [Previously Presented] An egress interface as claimed in claim 63, wherein the translation table is specific to a logical egress network port of the egress interface.

67. [Cancelled]

68. [Cancelled]

69. [Cancelled]

70. [Cancelled]

71. [Cancelled]

72. [Cancelled]

73. [Cancelled]

74. [Cancelled]

75. [Cancelled]

76. [Cancelled]

77. [Cancelled]

78. [Cancelled]

79. [Cancelled]

80. [Cancelled]

81. [Cancelled]

82. [Cancelled]

83. [Cancelled]

84. [Cancelled]

85. [Cancelled]